

ATTACHMENT B

Security Rules for SPARQ Users

The Department of Labor provides the SCSEP Performance and Results QPR (SPARQ) system to you subject to the following Security Rules. This policy may be updated periodically without notice. Any updates to the policy shall be effective immediately when posted. The most current version of this policy is available by clicking the Security Rules link on the SPARQ home page. This system is provided and operated by the United States Government. Following are the rules of behavior that users must adhere to when using SPARQ:

Unauthorized access or use of the system for any purpose other than official government business is punishable by a fine, imprisonment, or both. Your use of the system may be monitored (18 U.S. Code 1030).

You are entirely responsible for any and all activities that occur under your system account on the Web site.

Unauthorized attempts to upload information or change information on this Web site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996.

Only authorized users are allowed access to SPARQ data.

Data (printed or non-printed) must not be divulged to any individual who is not specifically authorized to receive such information.

Sharing user login information – i.e., your username and password – is strictly prohibited. You must take the necessary steps to ensure that others do not use your account to gain unauthorized access to this system.

Data must not be tampered with, changed, deleted, or altered unless the user is authorized to do so.

Data must not be disclosed without proper authorization from the management of the Office of Workforce Investment.

SPARQ may not be used to collect personal information (e.g., for mass mailing) or to conduct personal business without the consent of the U.S. Department of Labor. You are not allowed to use SPARQ to send commercial messages (e.g., advertisements) or unsolicited bulk emails (e.g., informational announcements such as loss of family notices).

Posting material or information that is unlawful or inappropriate, such as obscene materials, inappropriate content, or inappropriate language, on this site is prohibited. Users will be held solely responsible for any information posted and published to this Web site that is in violation of this policy. Users shall be held responsible for ensuring that any information or content posted/published is in fact appropriate for the intended recipient(s).

Any fraudulent activities, including illegally using someone else's account, posting system messages, or e-mailing customers for personal gain or concerns, is prohibited.

SPARQ may not be used to breach the security of any system user or to gain access to another person's (internal or external) computer, software, or data.

SPARQ may not be used in any attempt to circumvent the system authentication or security of any account, network, or host. Please note that this would include, but is not limited to, accessing data that is not intended for your information, logging into a server or account to which you are not authorized to gain access, or probing the security of other networks.

Using tools to compromise system security of SPARQ, such as password-guessing programs, cracking or packet sniffing tools, or any network probing tools, is strictly prohibited, and legal action may be taken against you if you use such tools.

Any attempt to disrupt or deny operation of SPARQ is strictly prohibited.

Transmitting viruses, via e-mail or otherwise, when using this system is not allowed.

It is prohibited to sell any of the data or information gained from SPARQ.

Users shall be responsible for notifying DOL's Office of Workforce Investment immediately of any unauthorized use of their account or any other breach of security in regards to these policies. DOL will investigate any and all suspected violations of these policies and reserves the right to take corrective or legal action against the violator. If an investigation is warranted, a user's account access may be disabled. As a system user, you are responsible for ensuring that your use of the system complies with the stated policies. **Any system user who does not agree to be bound by these policies should immediately discontinue use of this system and should notify DOL's Office of Workforce Investment.**

The rules outlined here must be followed by all system users of SPARQ. Any abuse of these policies may be punishable by law. Questions regarding complaints, violations, or the requirements of this policy should be directed to the National Office (SCSEP.National@dol.gov) for appropriate handling and resolution.

The Department of Labor, Employment and Training Administration, Office of Information Systems and Technology's Security Officer is responsible for supporting and enforcing the established policies set forth in these Security Rules. The policies set forth in the Security Rules have been put in place to protect SPARQ users from the adverse impact that can result from intentional violations of the rules. If you believe you have been the victim of activities that are in violation of the rules, the Office of Information Systems and Technology will take appropriate action to investigate and attempt to resolve the alleged violation. You may report your concern or incident to this division at the DOL Security and Emergency Management Office (SecurityOffice.DOL@dol.gov). Please make sure you include the date and time of the incident, log files (if appropriate), examples or any other information that may be useful to the investigation and verification of the incident, as well as your name and phone number or e-mail address so this office can contact you directly.

DOL reserves the right to disable your account access without notice for violation of these policies.

Certification by User:

I hereby certify that I have received a copy of the Security Rules for SPARQ Users and understand that my access to SPARQ is conditional upon my compliance with these rules.

Name

Date